The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
http://www.fiscal.treasury.gov/fsreports/fspia/fs_pia.htm

Name of System: Stored Value Card (SVC)

Document Version: 2.0

Document Date: May 1, 2014

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

SVC uses smart card technology with “electronic purses” to eliminate coin, currency, scrip, vouchers, money orders and other labor-intensive payment mechanisms in closed Government locations, such as military bases.

This program is aimed at eliminating the float loss associated with the more than $2 billion in coin and currency in circulation on military bases and other closed Government locations around the world. Stored value cards also eliminate the cost of securing, transporting, and accounting for cash held outside the Treasury. In addition, stored value cards eliminate the manually intensive back-end operations necessary to support scrip, vouchers, meal tickets, money orders, traveler’s checks, and other paper payment mechanisms used in closed Government environments.

Stored value cards are issued to military personnel and contractors, including merchants at selected Government sites. The cards may be issued in fulfillment of a Government payment, as is the case at select Army, Air Force, Navy and Marine Corps basic military training sites, where soldiers receive their initial payroll on stored value cards. Or, the cards may be issued without value so that cardholders can load funds onto them from their personal bank accounts. For example, at bases in Honduras, individuals can withdraw funds from their bank accounts in the United States to obtain a credit on their stored value card. Merchant locations on the Government sites, including stores and service providers, are equipped with stored value collection terminals so that cardholders can make purchases with the card.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Treasury/FMS.017 Collections Records

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
X no

4) Does this system contain any personal information about individuals?
X yes
__no

a. Is the information about members of the public?

Yes. Information is about active duty military personnel, military government contractor personnel, third country nationals, and government employees.

b. Is the information about employees or contractors?
Yes, see 4a.

5) What legal authority authorizes the purchase or development of this system?
5 U.S.C. 301; 31 U.S.C. 321; 31 U.S.C. chapter 33; 31 U.S.C. 3720

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
__ Employees
__ Contractors
__ Taxpayers
X Others (describe) Army, Air Force, Navy and Marine Corps basic trainees; deployed military personnel at selected overseas bases and troop transfer stations; civilians (contractors, including commercial/retail salespeople) at selected overseas bases and troop transfer stations.

2) Identify the sources of information in the system
Check all that apply:
__ Employee
X Public
X Federal agencies
__ State and local agencies
X Third party

a. What information will be collected from employees or contractors?
None

b. What information will be collected from the public?

SVC collects information from active duty military personnel and military government contractor personnel. Below is a description of the type of information SVC collects:

Social Security Number
First, Middle and Last Name
Banking Information
Mother's Maiden Name
Rank & Title
Date of Birth
Address

c. What Federal agencies are providing data for use in the system?

DFAS, United States Army Financial Management Command (USAFMCOM), U.S. Air Force Deputy Assistant Secretary for Financial Operations (SAF/FMP), U.S. Marine Corps (MCDOSS), U.S. Navy (NAVSUP).

First name, last name, address, social security number, telephone number, e-mail address, date of birth for all SVC cardholders. For SVC cardholders who use the Self-Service Kiosks, SVC also collects banking data (routing number, account number, account type).

d. What state and local agencies are providing data for use in the system?

None

e. From what other third party sources will data be collected?
None

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than Fiscal Service records, be verified for accuracy?

Information provided by DFAS for all EZpay program participants (basic military trainees) is output for SVC's use from the Military Pay records; this information has been verified by the appropriate service branch.

Information provided by EagleCash participants is input by the local base Finance Officer or their designated cashier(s) and, for military personnel, can be verified against Military Pay records and/or Military ID card (i.e. CAC).

b. How will data be checked for completeness?

Information provided by DFAS for all EZpay program participants (basic military trainees) is output for SVC's use from the Military Pay records; this information has been verified as complete by the appropriate service branch.

Information for EagleCash participants is input by the local base Finance Officer or their designated cashier(s); information for military personnel can be checked for completeness against Military Pay records and/or Military ID card (i.e. CAC).

c. What steps or procedures are taken to ensure the data is current?

For EZpay, the local Finance Office will send an updated file if information about the cardholder needs to be updated; the same holds true for EagleCash Finance Officers and cardholders. In addition, EagleCash Self-Service Kiosk users are instructed upon Kiosk enrollment to re-enroll at the Finance Office if their banking data changes. Lastly, if a Self-Service Kiosk user's banking data is determined to be out of date (i.e. transaction is returned via FedACH), the cardholder's card will be locked out of ACH transactions with a message referring the cardholder to the

Finance Office, and the local Finance Office is instructed separately to locate the cardholder and obtain up-to-date account information.

d. In what document(s) are the data elements described in detail?

All data elements are incorporated into the SVC database schema diagrams; these database schema diagrams are subsets of data collected from the field. Data is also kept on the electronic version of DD Form 2887 filled out by individual cardholders.

ATTRIBUTES OF THE DATA:

1) How is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The SVC Program uses the data collected to initiate debit and credit entries to the card holder's bank or credit union account. The cardholder completes a DD 2887 form in which authorizes the SVC program to conduct debit and credits to the cardholders account. It is necessary for the SVC program to collect the above mentioned information in order to process a SVC program transaction at any Self Service Kiosk or ACH-based laptop.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? How will this be maintained and filed?

The system tracks all smart card transactions for the individual cardholders. In this manner, there is additional information created about the cardholder/individual, in terms of their spending pattern while on base. This information is collected automatically, through the "processing" of SVC files received from Point of Sale (POS) devices, Self-Service Kiosks and Finance Office issuance stations/laptops; processing involves FRB receiving, collecting and uploading these transaction files into master databases for each of the two SVC programs. These transactions then create individual database records for each transaction performed; from this, the database can display a history via the back-office only, showing the spending patterns of the individual in question. Examples of reports that can be generated are: Card Transaction Detail History Report and Transaction Detail by Device Report. The Card Transaction Detail History Report will list all of the activity for a specific card and display the card number, cardholder's name, the date they were last on the warmlist, etc. The Transaction Detail by Device Report will list all of the cards and associated transaction amounts that were performed on a specific device.

This information is maintained electronically in a database.

3) Will the new data be placed in the individual's record?

Information about whether an SVC cardholder owes a debt as a result of use of the SVC program is exchanged with DFAS and/or Fed Debt in order to collect the debt from the pay of the cardholder who owes the debt.

If a cardholder meets a specific transactions criteria (i.e. credit load to a card), aggregate data derived from an SVC generated report will be sent to FinCEN in the form of a Suspicious Activity Report (SAR).

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?

N/A. The SVC does not make determinations about employees/public.

5) How will the new data be verified for relevance and accuracy?

Data populated in the reports is verified upon data input. In addition, once the reports are run, the report generator or program stakeholder reviews and confirms accuracy.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

The SVC program observes the principle of least privilege. All data is restricted based on a user's role and responsibility. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases themselves.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain)

The SVC program observes the principle of least privilege. All data is restricted based on a user's role and responsibility. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases themselves.

8) How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)

Information is retrieved by social security number or SVC card number at the direction of an operator, using an SVC Program application on an SVC workstation at the servicing Federal Reserve Bank. Information may also be retrieved by name. Information can also be displayed using SVC reporting service, or by viewing through a module of the SVC back-office system which only users with authority to view such information can do.

9) What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Reports produced include but are not limited to: Card Issuance (initial issuance or subsequent reloading of funds), Transaction History, and Kiosk activity. These reports are used primarily for internal use at the Federal Reserve Bank-FRB, either to reconcile a day's processing work or to assist with the research of an outstanding issue with a particular card. Reports are sent to SVC Program Managers, DFAS and to selected program-participating merchants. However, the data shared with these recipients varies (i.e. merchants only receive information about their own activity, not about individuals' issuance activity). In addition, the back-office system is only accessible to a limited number of authorized users from SVC – FRB employees or contractors, as well as Fiscal Service SVC Program Management Team.

10) What opportunities do individuals have to decline to provide information (i.e., in such cases where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses)? How can individuals grant consent?

Individuals are free to decline providing banking data for EagleCash card issuance; however, declining to provide this information will require that the user forego Self-Service Kiosk enrollment, as the information is required to process any Kiosk ACH-based transactions (i.e. Self-Service Card Load from Bank Account or Self-Service Card Unload to Bank Account). Further, individuals are not required to enroll in the EagleCash program. Upon enrollment for the EagleCash program, individuals sign an enrollment form (DD Form 2887) consenting to the use of their information for the EagleCash program.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

Data is retained indefinitely.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

N/A

3) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites?

N/A

**4) Is the system using technologies in ways that Fiscal Service has not previously employed
(e.g., monitoring software, Smart Cards, Caller-ID)?**

SVC uses smart card technology but is not using it in a new way that Fiscal Service has not previously employed.

5) **How does the use of this technology affect employee or public privacy?**
N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

An individual cardholder's transaction history allows for a system operator to review the location and dates/times of purchases over the lifecycle of that particular smartcard. The merchant location, date and time are recorded in each transaction record and are stored in the central database for that particular smartcard program. However, this data is not real-time; it is based on a time lag inherent in the system (which is offline, with batch processing), so there is no opportunity for real-time monitoring or tracking of individual cardholders.

7) **What kind of information is collected as a function of the monitoring of individuals?**

No data is collected specifically for the purpose of tracking or monitoring individuals; all data collected is required for the timely, accurate payment to merchants for sale activity, posting of funding transactions, Suspicious Activity Reporting (SAR) to FinCEN, etc. The ability to track or monitor individuals' purchase patterns (after the fact) is ancillary and may be used on an ad hoc basis by military law enforcement only where there is suspected fraudulent or unauthorized use of the card.

8) **What controls will be used to prevent unauthorized monitoring?**

Access to the SVC system is based on the principle of least privilege and limits access to individuals authorized specifically for the purpose of completing tasks and work related to SVC transaction processing, settlement or reconciliation (or support thereof). See Access to Data, below.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:
__ Contractors
__ Users
X Managers
X System Administrators
X System Developers
X Others (explain)_________

The following categories of individuals have access to the back-office system:

- Federal Reserve Bank SVC employees – staff at FRB designated to provide support for SVC processing/settlement/reconciliation, hardware deployment, server infrastructure management, software development, and business support functions

- FRB contractors – individuals under contract with FRB to provide support for SVC deployments or software testing/development

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is assigned based on the principle of least privilege; rights are assigned at the server/network infrastructure, database and application/function levels, with the smallest possible set of rights provided to each individual – the minimum required for them to perform their assigned duties.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

User access is restricted based on the principle of least privilege, as noted above.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Each SVC user with access to the back-end system is required to sign a Rules of Behavior document explaining the responsibilities inherent on all users of the system. This document also includes language specifically noting the appropriate disciplinary action for failure to comply with the Rules of Behavior. In addition, all users are undergo Security Awareness Training.

5) If contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

Yes. All contractor contracts contain a Non-Disclosure Agreement.

6) Do other systems share data or have access to the data in the system?
__yes
X no

If yes,

a. Explain the interface.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

7) Will other agencies share data or have access to the data in this system?
__yes
X no

If yes,

a. Check all that apply:
__Federal
__State
__ Local
__Other (explain) ___________________

b. Explain how the data will be used by the other agencies.

c. Identify the role responsible for assuring proper use of the data.